

BEST AVAILABLE COPY

DOCKET NO.: 259551US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideyuki SUZUKI

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP04/01076

INTERNATIONAL FILING DATE: February 3, 2004

FOR: BROADCAST ENCRYPTION KEY DISTRIBUTION SYSTEM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2003-026543	03 February 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/01076. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Surinder Sachar

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

RECEIVED

18 MAR 2004

WIPO PCT

日本国特許庁
JAPAN PATENT OFFICE

CT/JP2004/001076

03.2.2004

03 FEB 2005

10 Rec. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 2003年 2月 3日
Date of Application:

出願番号 特願2003-026543
Application Number:

[ST. 10/C] : [JP2003-026543]

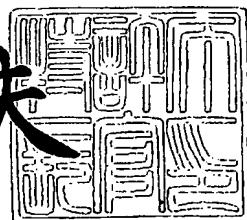
出願人 ソニー株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 3月 4日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2004-3016525

【書類名】 特許願
【整理番号】 0290800416
【提出日】 平成15年 2月 3日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/14

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 鈴木 英之

【特許出願人】

【識別番号】 000002185
【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100112955

【弁理士】

【氏名又は名称】 丸島 敏一

【手数料の表示】

【予納台帳番号】 172709
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0206900

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線アドホック通信システム、端末、その端末における復号方法、暗号化方法及びブロードキャスト暗号鍵配布方法並びにそれらの方法を端末に実行させるためのプログラム

【特許請求の範囲】

【請求項 1】 複数の端末により構成される無線アドホック通信システムであつて、

ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第1の端末と、

前記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第2の端末とを具備し、

前記第1の端末は前記第1の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、

前記第2の端末は前記第1の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号することを特徴とする無線アドホック通信システム。

【請求項 2】 前記第2の端末は、

前記第1の端末の端末識別子と前記第1の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、

受信したブロードキャストフレームの始点端末識別子に含まれる前記第1の端末の端末識別子により前記暗号鍵管理リストテーブルを検索して対応する前記第1の端末のブロードキャスト暗号鍵を抽出する手段と、

抽出された前記第1の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段とを備える

ことを特徴とする請求項1記載の無線アドホック通信システム。

【請求項 3】 前記第1の端末は、

前記第1の端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、

ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持された前記第1の端末のブロードキャスト暗号鍵により暗号化する手段と、

暗号化された前記ブロードキャストフレームを送信する手段とを備えることを特徴とする請求項1記載の無線アドホック通信システム。

【請求項4】 他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手段と、

抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段と
を具備することを特徴とする端末。

【請求項5】 他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵および前記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を暗号鍵として抽出し、前記受信したフレームの終点端末識別子がブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵を前記暗号鍵として抽出する手段と、

抽出された前記暗号鍵により前記フレームのペイロードを復号する手段と
を具備することを特徴とする端末。

【請求項6】 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、

ブロードキャストフレームのペイロードを前記ブロードキャスト暗号鍵により暗号化する手段と、

暗号化された前記ブロードキャストフレームを送信する手段と
を具備することを特徴とする端末。

【請求項 7】 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、

他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

送信しようとするフレームがブロードキャストフレームであれば前記生成鍵テーブルの前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、送信しようとする前記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵により前記ユニキャストフレームのペイロードを暗号化する手段と、

暗号化された前記フレームを送信する手段と
を具備することを特徴とする端末。

【請求項 8】 送信先端末のユニキャスト暗号鍵により自端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、
前記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を前記送信先端末に送信する手段と

を具備することを特徴とする端末。

【請求項 9】 他の端末の端末識別子に対応して前記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、

送信先端末のユニキャスト暗号鍵により前記暗号鍵管理リストを暗号化する手段と、
前記暗号化された暗号鍵管理リストを前記送信先端末に送信する手段と

を具備することを特徴とする端末。

【請求項 10】 他の端末から当該他の端末の端末識別子およびブロードキャスト暗号鍵を受信する手段と、
自端末のブロードキャスト暗号鍵により前記他の端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、

前記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵をブロードキャスト配布する手段と
を具備することを特徴とする端末。

【請求項11】 他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキャストフレームの復号方法であって

、
受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、

抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順と
を具備することを特徴とするブロードキャストフレームの復号方法。

【請求項12】 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロードキャストフレームの暗号化方法であって、

ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、

暗号化された前記ブロードキャストフレームを送信する手順と
を具備することを特徴とするブロードキャストフレームの暗号化方法。

【請求項13】 第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

第2の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、

前記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を前記第1の端末に送信する手順と
を具備することを特徴とする前記第2の端末におけるブロードキャスト暗号鍵配

布方法。

【請求項14】 第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

前記第1の端末の端末識別子およびブロードキャスト暗号鍵を第2の端末のブロードキャスト暗号鍵により暗号化する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を第3の端末に送信する手順と

を具備することを特徴とする前記第2の端末におけるブロードキャスト暗号鍵配布方法。

【請求項15】 他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末において、

受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、

抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順と

を端末に実行させることを特徴とするプログラム。

【請求項16】 自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、

ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、

暗号化された前記ブロードキャストフレームを送信する手順と
を端末に実行させることを特徴とするプログラム。

【請求項17】 第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信す

る手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

第2の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、

前記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を前記第1の端末に送信する手順と

を前記第2の端末に実行させることを特徴とするプログラム。

【請求項18】 第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、

前記第1の端末の端末識別子およびブロードキャスト暗号鍵を第2の端末のブロードキャスト暗号鍵により暗号化する手順と、

前記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を第3の端末に送信する手順と

を前記第2の端末に実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、無線アドホック通信システムに関し、特に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化して秘匿性を保つ無線アドホック通信システム、当該システムにおける端末、および、これらにおける処理方法ならびに当該方法をコンピュータ（端末）に実行させるプログラムに関する。

【0002】

【従来の技術】

電子機器の小型化、高性能化が進み、簡単に持ち運び利用することが可能とな

ったことから、必要になったその場で端末をネットワークに接続し、通信を可能とする環境が求められている。その一つとして、必要に応じて一時的に構築されるネットワーク、すなわち無線アドホックネットワーク技術の開発が進められている。この無線アドホックネットワークでは、特定のアクセスポイントを設けることなく、各端末（例えば、コンピュータ、携帯情報端末（PDA：Personal Digital Assistance）、携帯電話等）が自律分散して相互に接続される。このような無線アドホック通信システムにおいても、重要な情報の送受やプライベートなやりとりが第三者に傍受されることなく安心して行えるように暗号化等による秘匿性が求められている。

【0003】

一般に、通信内容を暗号化するためには、暗号化および復号化の両者で同じ共通鍵を用いる共通鍵暗号方式と、暗号化には公開鍵を用いて復号化には秘密鍵を用いる公開鍵暗号方式の二つの暗号方式が用いられている。共通鍵暗号方式は、暗号化および復号化を高速に行うことが可能であるが、通信の当事者同士が事前に何らかの方法で共通鍵を共有しておく必要がある。一方、公開鍵暗号方式は、共通鍵暗号方式に比べると処理が遅いが、当事者間同士で鍵を共有する必要がないという利点がある。そこで、共通鍵暗号の高速性と公開鍵暗号の利便性を組み合わせるハイブリッド方式が一般的に用いられている。具体的には、公開鍵暗号方式を用いて共通鍵を暗号化して送信し、当事者間で共有した共通鍵で実際の通信データの暗号化を行うことになる。

【0004】

この通信データの暗号化のための共通鍵は、用途に応じてユニキャスト暗号鍵とプロードキャスト暗号鍵とに分類される。ユニキャスト暗号鍵は、二つの端末間のユニキャスト通信において用いられるものであり、その二つの端末以外には知らされない共通鍵である。一方、プロードキャスト暗号鍵は、ある端末からのプロードキャスト通信を各端末において復号化するために用いられるものであり、プロードキャスト通信にかかる全ての端末間で共有される共通鍵である。従って、プロードキャスト暗号鍵は、ユニキャスト暗号鍵と比較して一般に、秘匿性を維持することが難しくなる。

【0005】

そのため、従来の通信システムにおいては、ブロードキャスト暗号鍵はネットワーク上の特定の装置において一元管理され、ブロードキャストグループにおけるブロードキャスト暗号鍵の秘匿性が図られている。例えば、モバイルデバイスに対してネットワーク所有者であるワイヤレスキャリアがブロードキャスト暗号鍵を予め設定しておくことにより、ブロードキャストメッセージを暗号化する技術が提案されている（例えば、特許文献1参照。）。

【0006】**【特許文献1】**

特表2002-501334号公報（図1）

【0007】**【発明が解決しようとする課題】**

従来の通信システムではブロードキャスト暗号鍵は一元管理されているが、無線アドホック通信システムにおいては端末は常に移動し、端末の参入および脱退が頻繁に行われ、ブロードキャストグループを構成する端末を固定することができない。また、無線媒体の性質上、そのような一元管理を行う装置への通信路が常に確保されているとは限らないため、一元管理に適さない。

【0008】

そこで、本発明の目的は、無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行うことにある。特に、本発明は、ネットワークを構成する全ての無線端末が管理情報（例えば、ビーコン等）を送信する無線ネットワークにおいて有用である。

【0009】**【課題を解決するための手段】**

上記課題を解決するために本発明の請求項1記載の無線アドホック通信システムは、複数の端末により構成される無線アドホック通信システムであって、ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第1の端末と、上記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第2の端末とを具備し、上記第1の

端末は上記第1の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを暗号化し、上記第2の端末は上記第1の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する。これにより、端末毎にブロードキャスト暗号鍵を自律分散して設定可能にするという作用をもたらす。

【0010】

また、本発明の請求項2記載の無線アドホック通信システムは、請求項1記載の無線アドホック通信システムにおいて、上記第2の端末が、上記第1の端末の端末識別子と上記第1の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、受信したブロードキャストフレームの始点端末識別子に含まれる上記第1の端末の端末識別子により上記暗号鍵管理リストテーブルを検索して対応する上記第1の端末のブロードキャスト暗号鍵を抽出する手段と、抽出された上記第1の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手段とを備える。これにより、ブロードキャストフレームの始点端末識別子に応じてブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【0011】

また、本発明の請求項3記載の無線アドホック通信システムは、請求項8記載の無線アドホック通信システムにおいて、上記第1の端末が、上記第1の端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持された上記第1の端末のブロードキャスト暗号鍵により暗号化する手段と、暗号化された上記ブロードキャストフレームを送信する手段とを備える。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【0012】

また、本発明の請求項4記載の端末は、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、受信したブロードキャストフレームの始点端

末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手段と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手段とを具備する。これにより、端末毎にブロードキャスト暗号鍵を自律分散して設定しておいて、ブロードキャストフレームの始点端末識別子に応じてブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【0013】

また、本発明の請求項5記載の端末は、他の端末の端末識別子に対応して上記他の端末との間のユニキャスト暗号鍵および上記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を暗号鍵として抽出し、上記受信したフレームの終点端末識別子がブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵を上記暗号鍵として抽出する手段と、抽出された上記暗号鍵により上記フレームのペイロードを復号する手段とを具備する。これにより、受信したフレームの終点端末識別子に応じてブロードキャスト暗号鍵およびユニキャスト暗号鍵を使い分けることを可能にするという作用をもたらす。

【0014】

また、本発明の請求項6記載の端末は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、ブロードキャストフレームのペイロードを上記ブロードキャスト暗号鍵により暗号化する手段と、暗号化された上記ブロードキャストフレームを送信する手段とを具備する。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【0015】

また、本発明の請求項7記載の端末は、自端末のブロードキャスト暗号鍵を保

持する生成鍵テーブルと、他の端末の端末識別子に対応して上記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、送信しようとするフレームがブロードキャストフレームであれば上記生成鍵テーブルの上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを暗号化し、送信しようとする上記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵により上記ユニキャストフレームのペイロードを暗号化する手段と、暗号化された上記フレームを送信する手段とを具備する。これにより、送信するフレームの終点端末識別子に応じてブロードキャスト暗号鍵およびユニキャスト暗号鍵を使い分けることを可能にするという作用をもたらす。

【0016】

また、本発明の請求項8記載の端末は、送信先端末のユニキャスト暗号鍵により自端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、上記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を上記送信先端末に送信する手段とを具備する。これにより、自端末のブロードキャスト暗号鍵を自端末の管理の下で配布するという作用をもたらす。

【0017】

また、本発明の請求項9記載の端末は、他の端末の端末識別子に対応して上記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、送信先端末のユニキャスト暗号鍵により上記暗号鍵管理リストを暗号化する手段と、上記暗号化された暗号鍵管理リストを上記送信先端末に送信する手段とを具備する。これにより、自端末の管理するブロードキャスト暗号鍵群（暗号鍵管理リスト）を自律分散して配布するという作用をもたらす。

【0018】

また、本発明の請求項10記載の端末は、他の端末から当該他の端末の端末識別子およびブロードキャスト暗号鍵を受信する手段と、自端末のブロードキャスト暗号鍵により上記他の端末の端末識別子およびブロードキャスト暗号鍵を暗号

化する手段と、上記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵をブロードキャスト配布する手段とを具備する。これにより、他の端末のブロードキャスト暗号鍵を自律分散して配布するという作用をもたらす。

【0019】

また、本発明の請求項11記載のブロードキャストフレームの復号方法は、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキャストフレームの復号方法であって、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手順と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手順とを具備する。これにより、ブロードキャストフレームの始点端末識別子に応じて復号化に使用するブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【0020】

また、本発明の請求項12記載のブロードキャストフレームの暗号化方法は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロードキャストフレームの暗号化方法であって、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、暗号化された上記ブロードキャストフレームを送信する手順とを具備する。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【0021】

また、本発明の請求項13記載のブロードキャスト暗号鍵配布方法は、第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、第2の端末の端末識別子およびブロードキャスト暗号

鍵を上記ユニキャスト暗号鍵により暗号化する手順と、上記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を上記第1の端末に送信する手順とを具備する。これにより、第1の端末と第2の端末との間で互いのブロードキャスト暗号鍵を配布するという作用をもたらす。

【0022】

また、本発明の請求項14記載のブロードキャスト暗号鍵配布方法は、第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、上記第1の端末の端末識別子およびブロードキャスト暗号鍵を第2の端末のブロードキャスト暗号鍵により暗号化する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を第3の端末に送信する手順とを具備する。これにより、第1の端末のブロードキャスト暗号鍵を第3の端末にブロードキャスト配布するという作用をもたらす。

【0023】

また、本発明の請求項15記載のプログラムは、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末において、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手順と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手順とを端末に実行させるものである。これにより、ブロードキャストフレームの始点端末識別子に応じて復号化に使用するブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【0024】

また、本発明の請求項16記載のプログラムは、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、暗号化された上記ブロードキャストフレームを送信する手

順とを端末に実行させるものである。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【0025】

また、本発明の請求項17記載のプログラムは、第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、第2の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により暗号化する手順と、上記暗号化された第2の端末の端末識別子およびブロードキャスト暗号鍵を上記第1の端末に送信する手順とを上記第2の端末に実行させるものである。これにより、第1の端末と第2の端末との間で互いのブロードキャスト暗号鍵を配布するという作用をもたらす。

【0026】

また、本発明の請求項18記載のプログラムは、第1の端末と第2の端末との間のユニキャスト暗号鍵により暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、上記第1の端末の端末識別子およびブロードキャスト暗号鍵を第2の端末のブロードキャスト暗号鍵により暗号化する手順と、上記暗号化された第1の端末の端末識別子およびブロードキャスト暗号鍵を第3の端末に送信する手順とを上記第2の端末に実行させるものである。これにより、第1の端末のブロードキャスト暗号鍵を第3の端末にブロードキャスト配布するという作用をもたらす。

【0027】

【発明の実施の形態】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【0028】

図1は、本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末300の構成例を示す図である。無線端末300は、通信処理

部320と、制御部330と、表示部340と、操作部350と、スピーカ360と、マイク370と、メモリ600とを備え、これらの間をバス380が接続する構成となっている。また、通信処理部320にはアンテナ310が接続されている。通信処理部320は、アンテナ310を介して受信した信号からネットワークインターフェース層（データリンク層）のフレームを構成する。また、通信処理部320は、ネットワークインターフェース層のフレームをアンテナ310を介して送信する。

【0029】

制御部330は、無線端末300全体を制御する。例えば、通信処理部320により構成されたフレームを参照して所定の処理を行う。また、制御部330は、タイマ335を有し、所定のイベントからの経過時間を計時する。表示部340は、所定の情報を表示するものであり、例えば、液晶ディスプレイ等が用いられ得る。操作部350は、無線端末300に対して外部から操作指示を行うためのものであり、例えば、キーボードやボタンスイッチ等が用いられ得る。スピーカ360は、音声を出力するものであり、無線端末300の利用者に対して注意を喚起したり他の端末と音声情報のやりとりを行うために用いられる。マイク370は、無線端末300に対して外部から音声入力を行うものであり、他の端末と音声情報のやりとりを行ったり操作指示を行うために用いられる。

【0030】

メモリ600は、属性証明書の発行端末に関する情報を保持する属性証明書発行端末リストテーブル610と、無線端末300自身のアクセス権限を示す属性証明書を保持する属性証明書テーブル620と、無線端末300自身の生成鍵に関する情報として自端末の公開鍵と秘密鍵と公開鍵証明書とブロードキャスト暗号鍵とを保持する生成鍵テーブル650と、他の端末との間のユニキャスト暗号鍵および他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストテーブル660とを格納する。

【0031】

図2は、本発明の実施の形態における属性証明書発行端末リストテーブル610の構成例である。この属性証明書発行端末リストテーブル610は、過去に属

性証明書を発行した実績のある端末に関する情報を保持するものであり、属性証明書発行端末の端末識別子 611 のそれぞれに対応して、公開鍵証明書 612 を保持している。端末識別子 611 は、ネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）における MAC (Media Access Control) アドレス等を用いることができる。公開鍵証明書 612 は、対応する端末識別子 611 により識別される端末の公開鍵証明書である。公開鍵証明書とは、証明書所有者（サブジェクト）の本人性を証明するものであり、証明書所有者の公開鍵を含む。この公開鍵証明書は証明書発行者たる認証局（CA: Certificate Authority）によって署名される。

【0032】

図3は、属性証明書発行端末リストテーブル 610 に保持される公開鍵証明書 612 のフォーマット 710 を示す図である。この公開鍵証明書のフォーマット 710 は、大きく分けて、署名前証明書 711 と、署名アルゴリズム 718 と、署名 719 とから構成される。署名前証明書 711 は、シリアル番号 712 と、発行者 714 と、有効期限 715 と、所有者 716 と、所有者 716 と、所有者公開鍵 717 を含む。

【0033】

シリアル番号 712 は、公開鍵証明書のシリアル番号であり、認証局によって採番される。発行者 714 は、公開鍵証明書の発行者たる認証局の名前である。この発行者 714 とシリアル番号 712 とにより公開鍵証明書は一意に識別される。有効期限 715 は、公開鍵証明書の有効期限である。所有者 716 は、公開鍵証明書の所有者の名前である。所有者公開鍵 717 は、所有者 716 の公開鍵である。

【0034】

署名 719 は公開鍵証明書に対する認証局による署名であり、署名アルゴリズム 718 はこの署名 719 のために使用された署名アルゴリズムである。署名アルゴリズムは、メッセージダイジェストアルゴリズムと公開鍵暗号アルゴリズムの2つにより構成される。メッセージダイジェストアルゴリズムは、ハッシュ関

数（要約関数）の一つであり、署名前証明書711のメッセージダイジェストを作成するためのアルゴリズムである。ここで、メッセージダイジェストとは、入力データ（署名前証明書711）を固定長のビット列に圧縮したものであり、拇指印や指紋（フィンガープリント）等とも呼ばれる。メッセージダイジェストアルゴリズムとしては、SHA-1 (Secure Hash Algorithm 1)、MD2 (Message Digest #2)、MD5 (Message Digest #5) 等が知られている。公開鍵暗号アルゴリズムは、メッセージダイジェストアルゴリズムにより得られたメッセージダイジェストを認証局の秘密鍵により暗号化するためのアルゴリズムである。この公開鍵暗号アルゴリズムとしては、素因数分解問題に基づくRSAや離散対数問題に基づくDSA等が知られている。このように、署名前証明書711のメッセージダイジェストを認証局の秘密鍵により暗号化したものが署名719となる。

【0035】

従って、この公開鍵証明書の署名719を認証局の公開鍵により復号することによってメッセージダイジェストが得られる。公開鍵証明書の利用者は、署名前証明書711のメッセージダイジェストを自身で作成し、それを認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、署名前証明書711の内容が改ざんされていないことを検証できる。

【0036】

図4は、属性証明書テーブル620に保持される属性証明書のフォーマット720を示す図である。この属性証明書は、大きく分けて、属性証明情報721と、署名アルゴリズム728と、署名729とから構成される。属性証明情報721は、所有者公開鍵証明書識別子723と、発行者724と、シリアル番号722と、有効期限725とを含む。

【0037】

所有者公開鍵証明書識別子723は、属性証明書の所有者の公開鍵証明書を識別するためのものである。具体的には、公開鍵証明書710（図3）の発行者714とシリアル番号712とにより識別する。発行者724は、属性証明書の発行者たる属性認証局（AA：Attribute certificate A

uthority) の名称である。シリアル番号 722 は、属性証明書のシリアル番号であり、属性証明書の発行者たる属性認証局によって採番される。このシリアル番号 722 と発行者 724 とにより属性証明書は一意に識別される。有効期限 725 は、属性証明書の有効期限である。

【0038】

署名 729 は属性証明書に対する属性認証局による署名であり、署名アルゴリズム 728 はこの署名 729 のために使用された署名アルゴリズムである。署名アルゴリズムの内容については、前述の公開鍵証明書の署名アルゴリズム 718 と同様であり、属性証明情報 721 のメッセージダイジェストを属性認証局の秘密鍵により暗号化したものが署名 729 となる。

【0039】

従って、この属性証明書の署名 729 を属性認証局の公開鍵により復号することによってメッセージダイジェストが得られる。属性証明書の利用者は、属性証明情報 721 のメッセージダイジェストを自身で作成し、それを属性認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、属性証明情報 721 の内容が改ざんされていないことを検証できる。

【0040】

なお、本明細書では、端末権限認証証明書の一例として属性証明書について説明するが、例えば、XML 言語等により端末権限を記述しておき、権限を有する機関がそれに署名を付することにより作成されたようなものであっても本発明における端末権限認証証明書として機能し得る。

【0041】

図 5 は、本発明の実施の形態における暗号鍵管理リストテーブル 660 の構成例である。この暗号鍵管理リストテーブル 660 は、復号化に用いられるブロードキャスト鍵および暗号化ならびに復号化に用いられるユニキャスト鍵を保持するものであり、他の端末の端末識別子 661 に対応して当該他の端末との間のユニキャスト暗号鍵 662 および当該他の端末のブロードキャスト暗号鍵 663 を保持する暗号鍵管理リストを少なくとも一つ有する。

【0042】

端末識別子 661 は、上述の通り他の端末を一意に識別するものであり、一例として MAC アドレス等を用いることができる。ユニキャスト暗号鍵 662 は、対応する端末識別子 661 を有する端末との間のユニキャスト通信のために定められた共通鍵である。このユニキャスト暗号鍵 662 を表すために、例えば、端末 A と端末 B との間で使用されるユニキャスト暗号鍵を「UK_AB」等と表記する。また、ブロードキャスト暗号鍵 663 は、対応する端末識別子 661 を有する端末がブロードキャスト通信を行うために定められた共通鍵である。このブロードキャスト暗号鍵 663 を表すために、例えば、端末 B からのブロードキャスト通信において使用されるブロードキャスト暗号鍵を「BK_B」等と表記する。

【0043】

なお、これらユニキャスト暗号鍵およびブロードキャスト暗号鍵に用いられる共通鍵アルゴリズムとしては、56ビットの鍵の長さを有するDES (Data Encryption Standard)、128ビット、192ビットおよび256ビットの3通りの鍵の長さを有するAES (Advanced Encryption Standard) 等が知られている。

【0044】

図6は、本発明の実施の形態におけるブロードキャスト暗号鍵およびユニキャスト暗号鍵の機能を示す図である。ブロードキャスト暗号鍵は、ブロードキャスト通信を行う各端末毎に定められるものであり、ブロードキャスト送信端末における暗号化およびブロードキャスト受信端末における復号化の両者で共通に用いられる共通鍵である。例えば、端末 A のブロードキャスト暗号鍵 (BK_A) は、端末 A がブロードキャスト通信を送信する際の暗号化に使用され、端末 A 以外の端末が端末 A からのブロードキャスト通信を受信する際の復号化に使用される。

【0045】

一方、ユニキャスト暗号鍵は、端末対毎に定められるものであり、端末対における通信の暗号化および復号化の両者で共通に用いられる共通鍵である。例えば、端末 A と端末 B の間のユニキャスト暗号鍵 (UK_AB) は、端末 A が端末 B

にユニキャスト通信を送信する際の暗号化および端末Bが端末Aからのユニキャスト通信を受信する際の復号化に使用されるだけでなく、端末Bが端末Aにユニキャスト通信を送信する際の暗号化および端末Aが端末Bからのユニキャスト通信を受信する際の復号化にも使用される。

【0046】

図7は、本発明の実施の形態における経路テーブル680の構成例である。この経路テーブル680は、終点端末にフレームを到達させるための転送先端末に関する情報を保持するものであり、終点端末の端末識別子681に対応してフレームの転送先端末の端末識別子682および有効時間683を保持する経路リストを少なくとも一つ有する。

【0047】

終点端末識別子681および転送先端末識別子682における端末識別子は、上述の通り他の端末を一意に識別するものである。ある端末に最終的にフレームを配達するために、次にどの端末にフレームを転送すべきであるかを示している。

【0048】

無線アドホック通信システムにおいては、ネットワーク構成が時々刻々と変化する可能性がある。従って、経路テーブル680に保持される情報も古くなる可能性がある。そこで、有効時間683によって、対応する情報の鮮度を管理する。例えば、情報更新時もしくは情報更新からの経過時間を有効時間683に記録していくことにより、所定時間以上経過した情報を削除もしくは更新することが考えられる。これらの時間を計時するために制御部330のタイマ335が使用される。

【0049】

図8は、本発明の実施の形態におけるブロードキャスト通信およびユニキャスト通信に用いられるフレーム構成を示す図である。フレーム800は、ヘッダ部801と、ペイロード部802とから構成される。また、ヘッダ部801は、始点端末識別子803と、終点端末識別子804と、送信端末識別子805と、受信端末識別子806と、フレーム種別807と、属性証明書の有無808とを含

む。始点端末識別子 803 は、このフレームを最初に発信した端末の端末識別子である。なお、端末識別子は、前述のようにネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）における MAC アドレス等を用いることができる。終点端末識別子 804 は、このフレームの最終宛先の端末の端末識別子である。

【0050】

送信端末識別子 805 および受信端末識別子 806 は、フレームを中継する際に用いられる。無線アドホック通信システムにおいては、ネットワーク内の全ての端末が直接通信できるとは限らず、電波の届かない端末へフレームを送信したい場合には他の端末を介してマルチホップにより通信経路を確立しなければならない。この場合にフレームの送受信を行う端末間で使用されるのが送信端末識別子 805 および受信端末識別子 806 である。フレーム種別 807 は、フレームの種別を示すものである。

【0051】

ペイロード部 802 には通信の内容であるデータ 809 が格納される。このペイロード部 802 が、ユニキャスト暗号鍵およびブロードキャスト暗号鍵による暗号化および復号化の対象となる。

【0052】

次に本発明の実施の形態における無線アドホック通信システムの動作について図面を参照して説明する。本発明の実施の形態では、端末がネットワーク資源に接続する際に端末間で属性証明書を用いて相互認証（図 9）を行い、互いの認証に成功した後にセッション鍵の配布、ユニキャスト暗号鍵の生成、および、ブロードキャスト暗号鍵の配布を行う（図 13）。これら図 9 および図 13 における各処理は、無線端末 300 における制御部 330 により実現される。

なお、相互認証に用いられる属性証明書は、予め適切に発行されて、各端末の属性証明書テーブル 620（図 1）に保持されていることを前提とする。また、属性証明書の検証に必要な属性証明書発行端末の公開鍵は、各端末の属性証明書発行端末リストテーブル 610 の公開鍵証明書 612（図 2）に予め設定されていることを前提とする。

【0053】

図9は、本発明の実施の形態における相互認証の手順を示す図である。本発明の実施の形態における無線アドホック通信システムでは、各端末は定期的にビーコンを送信し、他の端末に対して自己の存在を知らせる。以下では、端末Bのビーコンをトリガーとして端末Aが認証要求を行うものと仮定するが、最終的に相互に認証が行われればよく、何れの端末のビーコンをトリガーとしてもよい。

【0054】

まず、端末Bが、ビーコン2111を送信しているものとする(211)。このビーコン2111のフレーム構成は図10の通りである。ビーコンフレーム810は、図8で説明したフレーム800の構成に基づくものであり、ヘッダ部811およびペイロード部812に分けられる点も同様である。各端末識別子813乃至816も図8の各端末識別子803乃至806と同様である。ビーコンフレーム810では、終点端末識別子814にはブロードキャストアドレス(例えば、全てのビットに1)が設定される。フレーム種別817は、ここでは、ビーコンフレームであることを示す。属性証明書の有無818は、ネットワーク資源にアクセスする権限を示す属性証明書をビーコンフレームの送信元端末が有しているか否かを示すものである。属性証明書を有していない旨をこの属性証明書の有無818が示している場合には、相互認証を進めることはできず、例えば、属性証明書の取得を促す等の処置を探ることが考えられる。

【0055】

端末Aは、端末Bから送信されたビーコン2111を受信すると(111)、ビーコンフレーム810の属性証明書の有無818をチェックする。端末Bが属性証明書を有していると判断すると、端末Aは端末Bに対して端末Aを認証するよう認証要求メッセージ1122を送信する(112)。この認証要求メッセージ1122のフレーム構成は図11の通りである。認証要求フレーム870は、図8で説明したフレーム800の構成に基づくものであり、ヘッダ部871およびペイロード部872に分けられる点も同様である。各端末識別子873乃至876も図8の各端末識別子803乃至806と同様である。フレーム種別877は、ここでは、認証要求フレームであることを示す。

【0056】

また、この認証要求フレーム870では、ペイロード部872のデータ879として、送信元である端末Aの公開鍵証明書8791および属性証明書8792が含まれる。端末Aの公開鍵証明書8791は端末Aの生成鍵テーブル650に予め格納されたものであり、端末Aの属性証明書8792は端末Aの属性証明書テーブル620に予め格納されたものである。

【0057】

端末Bは、端末Aから送信された認証要求メッセージ1122を受信すると、その内容から端末Aを認証する（212）。具体的には、属性証明書発行端末リストテーブル610の公開鍵証明書612（図2）から属性認証局の公開鍵を抽出して、この公開鍵によって認証要求メッセージ1122に含まれる属性証明書8792の署名729（図4）を復号することにより署名時のメッセージダイジェストを得る。そして、属性証明書8792の属性証明情報721（図4）のメッセージダイジェストを新たに生成する。この新たに生成されたメッセージダイジェストが署名時のメッセージダイジェストと一致していることを確認する。もしこれらが一致しないとすれば、属性証明書は署名後に改ざんされた可能性があり、属性証明書の検証は失敗となる。両者が一致している場合には、さらに認証要求メッセージ1122に含まれる属性証明書8792の所有者公開鍵証明書識別子723（図4）が、認証要求メッセージ1122に含まれる公開鍵証明書8791の発行者714およびシリアル番号712（図3）に一致することを確認する。これが一致すれば、公開鍵証明書の所有者である端末Aは属性証明書の所有者であることが確認できる。もしこれらが一致しなければ、属性証明書の所有者は端末Aではなく、属性証明書の検証は失敗となる。

【0058】

端末Aの認証（212）に成功すると、端末Bは端末Aの認証に成功したことを見せる認証成功メッセージ2131を端末Aに送信する（213）。この認証成功メッセージ2131の認証応答フレーム構成は図12の通りである。認証応答フレーム880は、図8で説明したフレーム800の構成に基づくものであり、ヘッダ部881およびペイロード部882に分けられる点も同様である。各

端末識別子883乃至886も図8の各端末識別子803乃至806と同様である。認証成功メッセージ2131の場合、フレーム種別887は認証成功フレームとなる。この認証応答フレーム880では、さらに応答理由種別888を含むが、認証成功の場合は特に必要はない。

【0059】

なお、端末Aの属性証明書の検証（212）に失敗すると、端末Bは端末Aの認証に成功したことを見せる認証失敗メッセージを端末Aに送信することになる。この認証失敗メッセージの認証応答フレーム構成は図12により説明した通りである。但し、認証失敗メッセージの場合、フレーム種別887は認証失敗フレームとなり、応答理由種別888には認証に失敗した理由として属性証明書のメッセージダイジェスト不一致、属性証明書失効等の事由がコード化されて示される。これら。認証成功メッセージ2131または認証失敗メッセージは端末Aにおいて受信されて確認される（113）。

【0060】

端末Aの属性証明書の検証（212）に成功すると、さらに端末Bは端末Aに対して端末Bを認証するよう認証要求メッセージ2141を送信する（214）。この認証要求メッセージ2141のフレーム構成は上述の図11と同様であり、送信元である端末Bの公開鍵証明書8791および属性証明書8792が含まれる。

【0061】

端末Aは、端末Bから送信された認証要求メッセージ2141を受信すると、その内容から端末Bを認証する（114）。この認証の内容は、既に説明した端末Bにおける端末Aの認証（212）と同様であり、属性証明書の検証、および、属性証明書の所有者の確認等を行う。

【0062】

端末Bの認証（212）に成功すると、端末Aは端末Bの認証に成功したことを見せる認証成功メッセージ1152を端末Bに送信する（115）。この認証成功メッセージ1152の認証応答フレーム構成は上述の図12と同様である。また、端末Bの属性証明書の検証（212）に失敗した場合には、端末Aは端

末Bの認証に成功したことを通知する認証失敗メッセージを端末Bに送信することになる。この認証失敗メッセージの認証応答フレーム構成も図12により説明した通りである。これら認証成功メッセージ1152または認証失敗メッセージは端末Bにおいて受信されて確認される(215)。

【0063】

このようにして、端末Aおよび端末Bにおいて互いの端末の認証に成功すると相互認証は完了し、次に暗号鍵の配布を行う。

【0064】

図13は、本発明の実施の形態における暗号鍵配布の手順を示す図である。ここで、端末A(100)は新規にネットワークに参入しようとしている端末であり、端末B(200)は既にネットワークに参入している属性証明書発行端末である。

【0065】

まず、端末Aは、端末Bとの間で通信を行うためのセッション鍵を生成する(121)。このセッション鍵は、端末Aと端末Bとの間の共通鍵であり、乱数を用いて生成することができる。端末Aは、このセッション鍵を端末Bの公開鍵により暗号化してセッション鍵配布メッセージ1222として端末Bに送信する(122)。このセッション鍵配布メッセージ1222のセッション鍵配布フレーム構成は図14の通りである。セッション鍵配布フレーム820は、図8で説明したフレーム800の構成に基づくものであり、ヘッダ部821およびペイロード部822に分けられる点も同様である。各端末識別子823乃至826も図8の各端末識別子803乃至806と同様である。フレーム種別827はセッション鍵配布フレームとなる。ペイロード部822のデータ829にはセッション鍵8291が含まれる。

【0066】

なお、このセッション鍵配布フレームのペイロード部822は、ユニキャスト暗号鍵またはブロードキャスト暗号鍵による暗号化または復号化の対象とはならず、受信端末の公開鍵で暗号化され、受信端末の秘密鍵で復号化される。端末Aは、相互認証の段階で端末Bの公開鍵証明書を受信しているため、その所有者公

開鍵 717 (図3) により端末Bの公開鍵を得ることができる。

【0067】

端末Bは、端末Aから送信されたセッション鍵配布メッセージ1222を受信すると、セッション鍵8291を端末Bの秘密鍵により復号化する(222)。これにより、端末Aおよび端末Bの間で同一のセッション鍵を共有したことになる。

【0068】

その後、端末Aおよび端末Bは、セッション鍵からユニキャスト暗号鍵(UK_AB)を生成する(123、223)。このユニキャスト暗号鍵は、セッション鍵をそのまま利用してもよく、また、このセッション鍵を種(シード)としてハッシュ関数により新たにユニキャスト暗号鍵を生成するようにしてもよい。このようにして得られた端末Aと端末Bとの間のユニキャスト暗号鍵(UK_AB)は、両端末の暗号鍵管理リストテーブル660の対応するユニキャスト暗号鍵662(図5)に格納される。

【0069】

次に、端末Aは、予め生成していた端末Aのブロードキャスト暗号鍵(BK_A)と端末Aの端末識別子との対を端末Bとの間のユニキャスト暗号鍵(UK_AB)により暗号化してブロードキャスト鍵配布メッセージ1242として端末Bに送信する(124)。このブロードキャスト鍵配布メッセージ1242のブロードキャスト鍵配布フレーム構成は図15の通りである。ブロードキャスト鍵配布フレーム830は、図8で説明したフレーム800の構成に基づくものであり、ヘッダ部831およびペイロード部832に分けられる点も同様である。各端末識別子833乃至836も図8の各端末識別子803乃至806と同様である。フレーム種別837はブロードキャスト鍵配布フレームとなる。ペイロード部832のデータ839には端末識別子8391とブロードキャスト暗号鍵8392との対が含まれる。端末Aは、端末Aのブロードキャスト暗号鍵(BK_A)8392を生成鍵テーブル650に保持している。また、ブロードキャスト鍵配布メッセージ1242のペイロード部832の暗号化に用いるユニキャスト暗号鍵(UK_AB)は暗号鍵管理リストテーブル660のユニキャスト暗号鍵6

62 (図5) に保持している。

【0070】

端末Bは、端末Aからブロードキャスト鍵配布メッセージ1242を受信すると、ブロードキャスト鍵配布メッセージ1242のペイロード部832を端末Aとの間のユニキャスト暗号鍵 (UK_AB) により復号化する (224)。これにより、端末Aのブロードキャスト暗号鍵と端末識別子とを取得する。そして、この端末Aのブロードキャスト暗号鍵を端末Aの端末識別子と関連付けて、暗号鍵管理リストテーブル660のブロードキャスト暗号鍵663 (図5) に格納する。

【0071】

そして、端末Bは、端末Aのブロードキャスト暗号鍵 (BK_A) と端末Aの端末識別子との対を端末Bのブロードキャスト暗号鍵 (BK_B) により暗号化してブロードキャスト鍵配布メッセージ2244として他の端末にブロードキャスト送信する (225)。このブロードキャスト鍵配布メッセージ2244のブロードキャスト鍵配布フレーム構成は上述した図15の通りであるが、終点端末識別子834にはブロードキャストアドレス (例えば、全てのビットに1) が設定される。

【0072】

端末Bからのブロードキャスト鍵配布メッセージ2244を受信した他の端末400 (例えば、端末Cや端末D) は、ブロードキャスト鍵配布メッセージ2244のペイロード部832を端末Bのブロードキャスト暗号鍵 (BK_B) により復号化する (425)。これにより、端末Aのブロードキャスト暗号鍵と端末識別子とを取得する。そして、この端末Aのブロードキャスト暗号鍵を端末Aの端末識別子と関連付けて、暗号鍵管理リストテーブル660のブロードキャスト暗号鍵663 (図5) に格納する。

【0073】

さらに、端末Bは、端末Bの暗号鍵管理リストテーブル660に含まれるブロードキャスト暗号鍵663の全てをそれぞれの端末識別子661と対にして、端末Aとの間のユニキャスト暗号鍵 (UK_AB) により暗号化してブロードキャ

スト鍵配布メッセージ2261として端末Aに送信する（226）。このブロードキャスト鍵配布メッセージ2261のブロードキャスト鍵配布フレーム構成は上述した図15の通りであるが、ペイロード部832には端末識別子8391およびブロードキャスト暗号鍵8392の対が複数含まれる可能性がある。

【0074】

端末Bからブロードキャスト鍵配布メッセージ2261を受信した端末Aは、ブロードキャスト鍵配布メッセージ2261のペイロード部832を端末Bとの間のユニキャスト暗号鍵（UK_AB）により復号化する（126）。これにより、他の端末のブロードキャスト暗号鍵と端末識別子との対を取得する。そして、これら他の端末のブロードキャスト暗号鍵をそれぞれの端末の端末識別子と関連付けて、暗号鍵管理リストテーブル660のブロードキャスト暗号鍵663（図5）に格納する。

【0075】

次に本発明の実施の形態における無線アドホック通信システムの各端末の暗号鍵選択アルゴリズムについて図面を参照して説明する。

【0076】

図16は、本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。図8のフレームにおいて、ブロードキャストフレームでは終点端末識別子804がブロードキャストアドレスである（ステップS921）、自端末のブロードキャスト暗号鍵によりペイロード部802を暗号化する（ステップS922）。一方、ブロードキャストフレームでなければ終点端末識別子804がブロードキャストアドレス以外である（ステップS921）、終点端末識別子804と一致する端末識別子661に対応するユニキャスト暗号鍵662を図5の暗号鍵管理リストテーブル660から抽出して、そのユニキャスト暗号鍵によりペイロード部802を暗号化する（ステップS923）。その後、暗号化されたフレームは下位層に送出される（ステップS924）。

【0077】

図17は、本発明の実施の形態におけるフレーム受信の際の暗号鍵選択アルゴリズムを示す図である。図8のフレームにおいて、終点端末識別子804がブロ

ードキャストアドレスであれば（ステップS911）、始点端末識別子803と一致する端末識別子661に対応するブロードキャスト暗号鍵663を図5の暗号鍵管理リストテーブル660から抽出して、そのブロードキャスト暗号鍵によりペイロード部802を復号化する（ステップS912）。

【0078】

終点端末識別子804がブロードキャストアドレスでなく（ステップS911）、自端末の端末識別子であれば（ステップS913）、始点端末識別子803と一致する端末識別子661に対応するユニキャスト暗号鍵662を図5の暗号鍵管理リストテーブル660から抽出して、そのユニキャスト暗号鍵によりペイロード部802を復号化する（ステップS914）。ステップS912またはステップS914において復号化されたフレームは上位層において処理される（ステップS915）。

【0079】

一方、終点端末識別子804がブロードキャストアドレスでなく（ステップS911）、自端末の端末識別子でもなければ（ステップS913）、そのフレームは次点の端末へ転送される（ステップS916）。次点の端末は、フレーム800の終点端末識別子804（図8）と一致する終点端末識別子681を経路テーブル680（図7）から抽出して、対応する転送先端末識別子682を参照することにより知ることができる。

【0080】

このように、本発明の実施の形態によれば、暗号鍵管理リストテーブル660において端末識別子661に関連付けてブロードキャスト暗号鍵663を保持しておくことにより、端末毎に異なるブロードキャスト暗号鍵を適用することができる。これらブロードキャスト暗号鍵は、ブロードキャスト通信を行う端末自身が生成して図13のシーケンス等を用いて配布するものである。従って、無線アドホック通信システムのようにブロードキャスト暗号鍵の一元管理が適さない環境において、ブロードキャスト暗号鍵の管理を各端末において自律分散して行うことができる。

【0081】

なお、本発明の実施の形態は、ネットワークに属する全ての端末へ均等に配送するブロードキャストに関するものであるが、この「ブロードキャスト」の語句は厳格に解釈されるものではなく、「マルチキャスト」を含む広い概念として解釈されるべきものである。

【0082】

また、ここでは本発明の実施の形態を例示したものであり、本発明はこれに限られず、本発明の要旨を逸脱しない範囲において種々の変形を施すことができる。

【0083】

また、ここで説明した処理手順はこれら一連の手順を有する方法として捉えてもよく、これら一連の手順をコンピュータに実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。

【0084】

【発明の効果】

以上の説明で明らかのように、本発明によると、無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行うことができるという効果が得られる。

【図面の簡単な説明】

【図1】

本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末300の構成例を示す図である。

【図2】

本発明の実施の形態における属性証明書発行端末リストテーブル610の構成例を示す図である。

【図3】

本発明の実施の形態における属性証明書発行端末リストテーブル610に保持される公開鍵証明書612のフォーマット710を示す図である。

【図4】

本発明の実施の形態における属性証明書テーブル620に保持される属性証明

書のフォーマット720を示す図である。

【図5】

本発明の実施の形態における暗号鍵管理リストテーブル660の構成例を示す図である。

【図6】

本発明の実施の形態におけるブロードキャスト暗号鍵およびユニキャスト暗号鍵の機能を示す図である。

【図7】

本発明の実施の形態における経路テーブル680の構成例を示す図である。

【図8】

本発明の実施の形態におけるブロードキャスト通信およびユニキャスト通信に用いられるフレーム構成を示す図である。

【図9】

本発明の実施の形態における相互認証の手順を示す図である。

【図10】

本発明の実施の形態におけるビーコンフレーム810の構成例を示す図である

。

【図11】

本発明の実施の形態における認証要求フレーム870の構成例を示す図である

。

【図12】

本発明の実施の形態における認証応答フレーム880の構成例を示す図である

。

【図13】

本発明の実施の形態における暗号鍵配布の手順を示す図である。

【図14】

本発明の実施の形態におけるセッション鍵配布フレーム820の構成例を示す図である。

【図15】

本発明の実施の形態におけるプロードキャスト鍵配布フレーム830の構成例を示す図である。

【図16】

本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。

【図17】

本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。

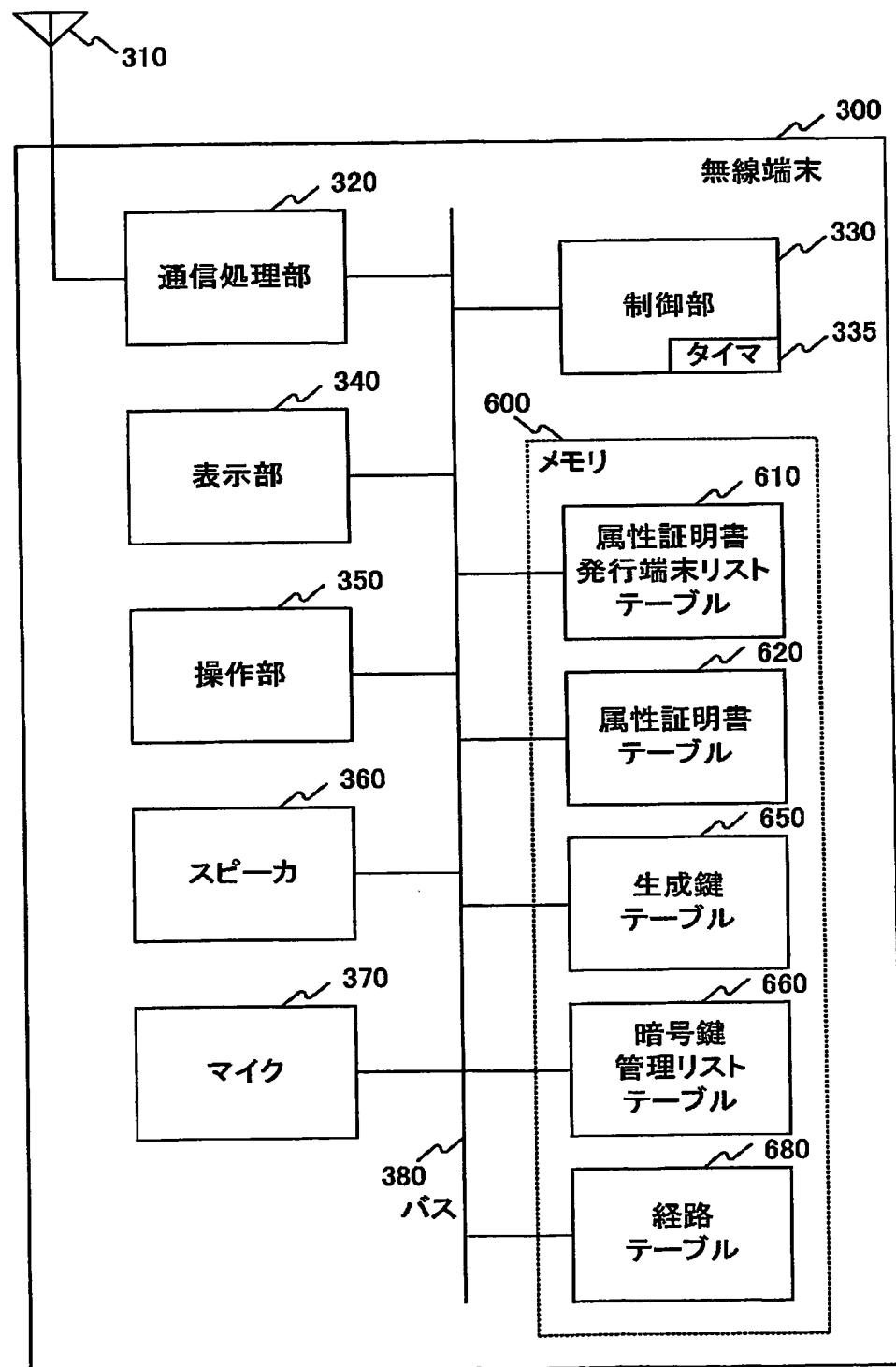
【符号の説明】

- 300 無線端末
- 310 アンテナ
- 320 通信処理部
- 330 制御部
- 335 タイマ
- 340 表示部
- 350 操作部
- 360 スピーカ
- 370 マイク
- 380 バス
- 400 端末
- 600 メモリ
- 610 属性証明書発行端末リストテーブル
- 620 属性証明書テーブル
- 650 生成鍵テーブル
- 660 暗号鍵管理リストテーブル
- 680 経路テーブル
- 710 公開鍵証明書
- 720 属性証明書
- 800 フレーム

- 810 ピーコンフレーム
- 820 セッション鍵配布フレーム
- 830 ブロードキャスト鍵配布フレーム
- 870 認証要求フレーム
- 880 認証応答フレーム

【書類名】 図面

【図 1】



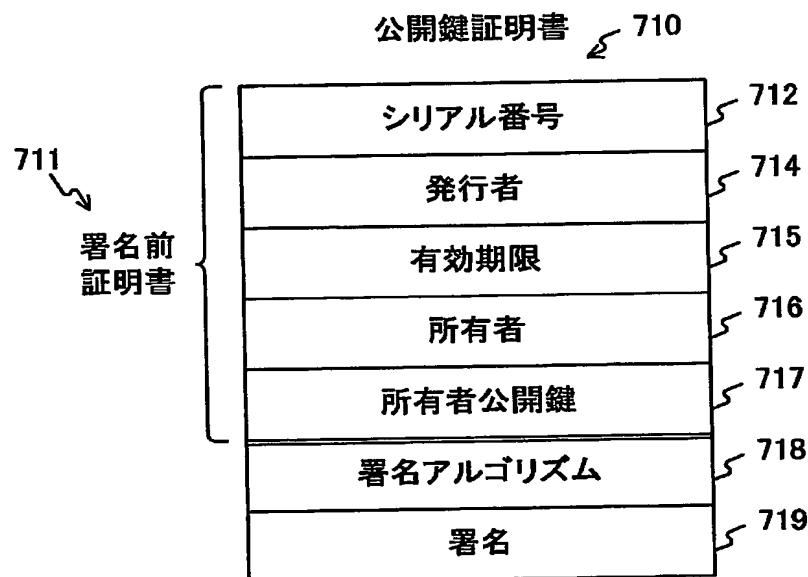
【図2】

属性証明書発行端末リストテーブル 610

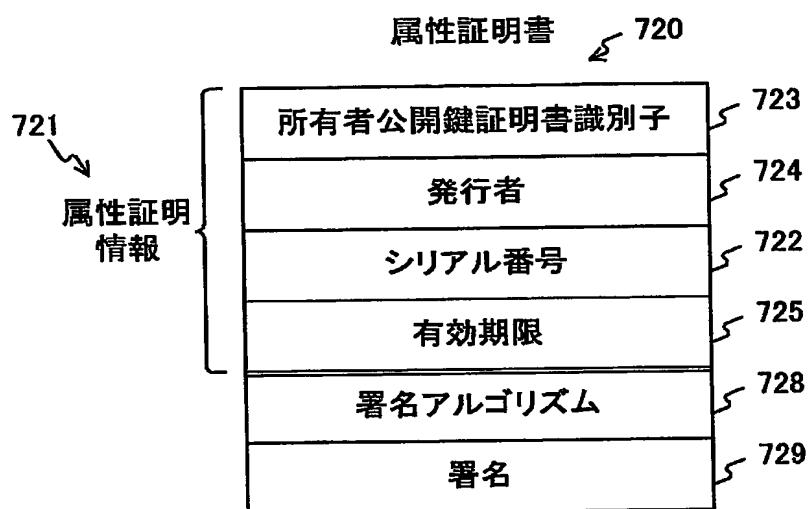
端末識別子 611 公開鍵証明書 612

端末X	公開鍵証明書X
端末Y	公開鍵証明書Y

【図3】



【図4】



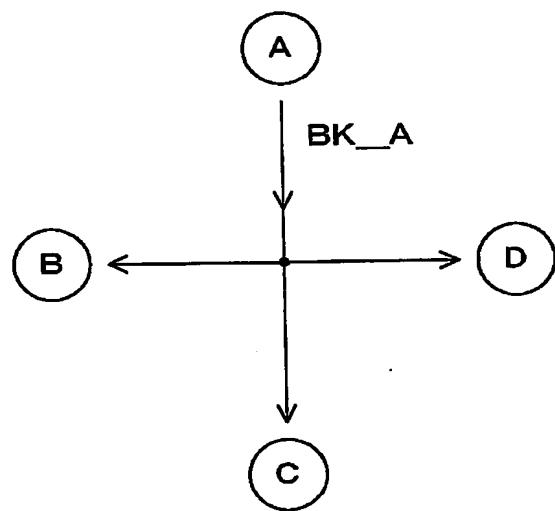
【図 5】

暗号鍵管理リストテーブル 660

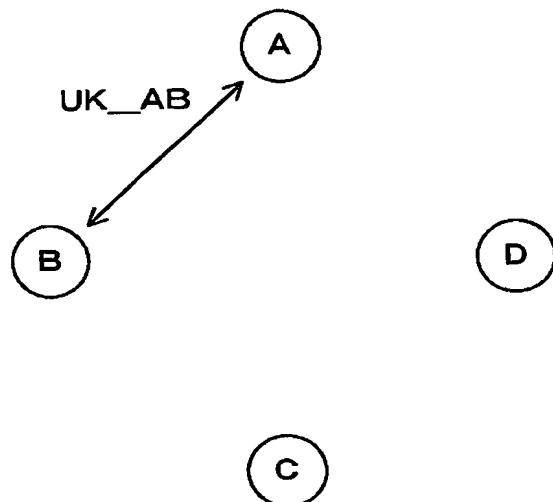
端末識別子 661 ユニキャスト暗号鍵 662 ブロードキャスト暗号鍵 663

端末B	UK_AB	BK_B
端末C	UK_AC	BK_C
端末D	UK_AD	BK_D
⋮	⋮	⋮

【図6】



(a) ブロードキャスト鍵



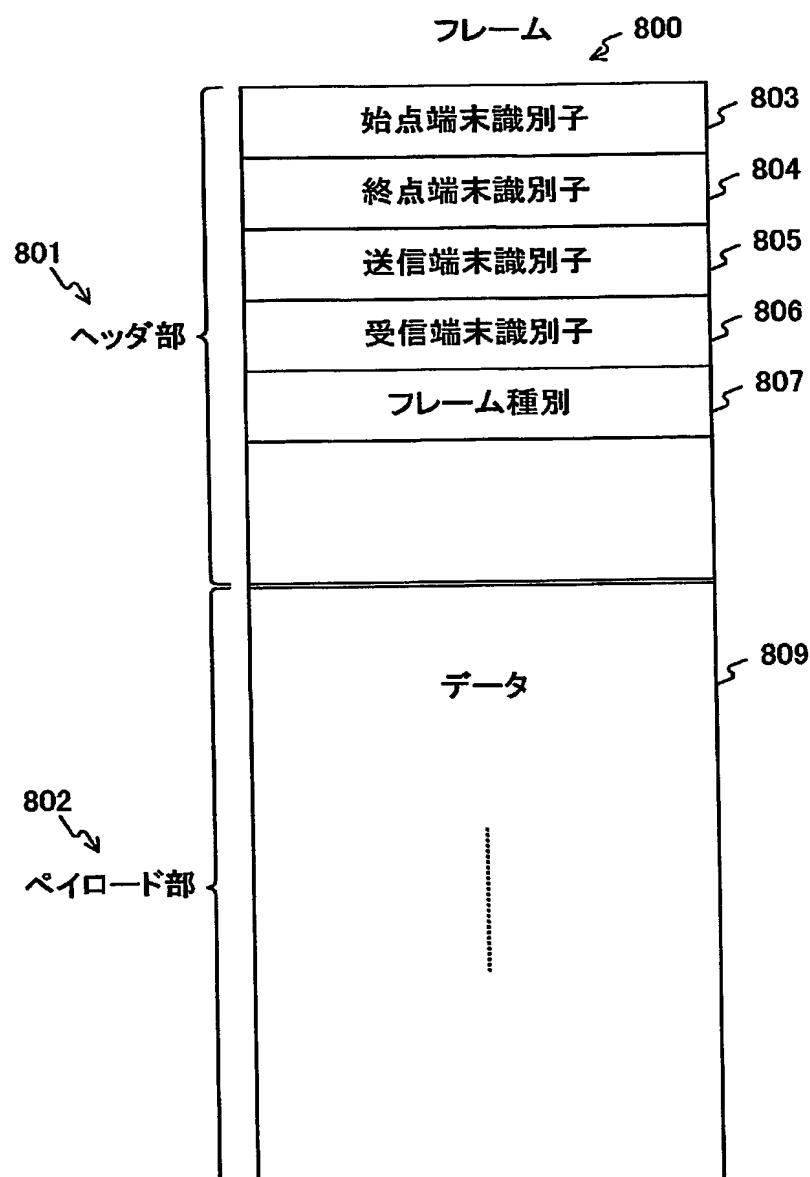
(b) ユニキャスト鍵

【図7】

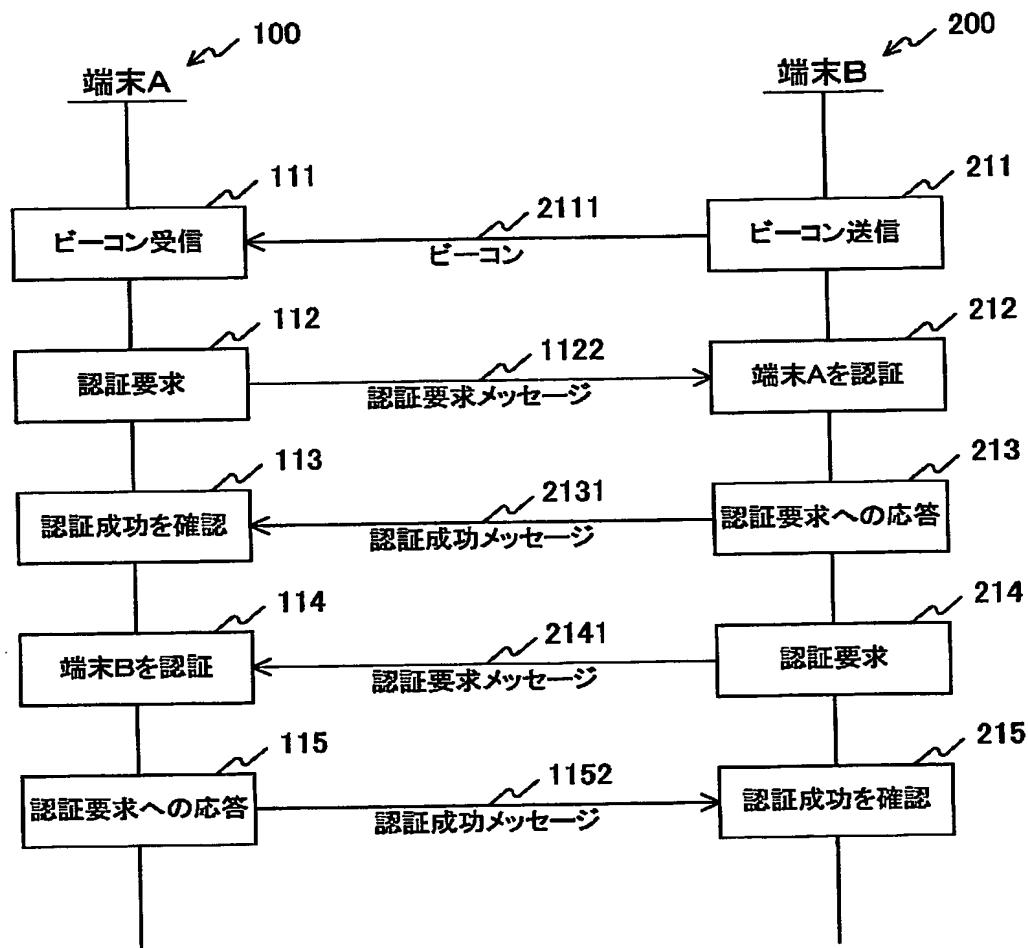
経路テーブル

終点端末識別子	転送先端末識別子	有効時間
端末B	端末B	1:30
端末C	端末B	0:50
端末D	端末B	0:30
⋮	⋮	⋮

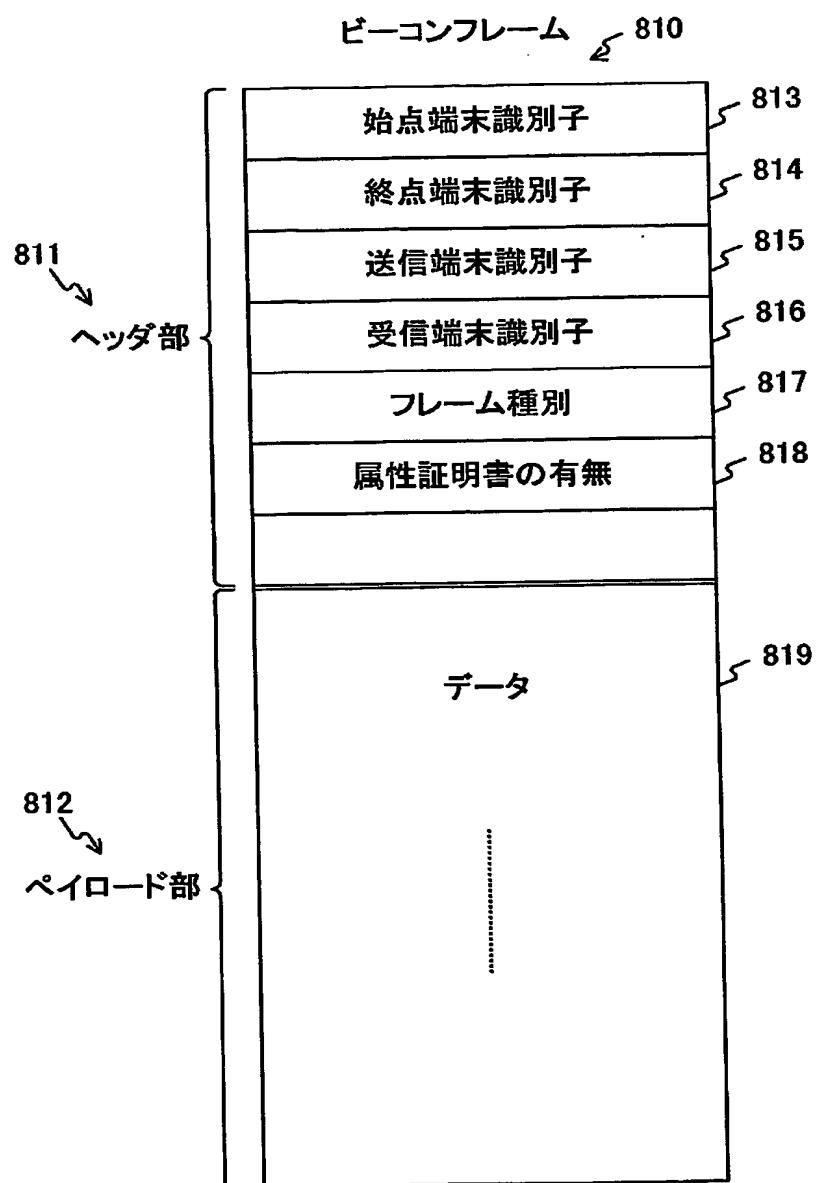
【図8】



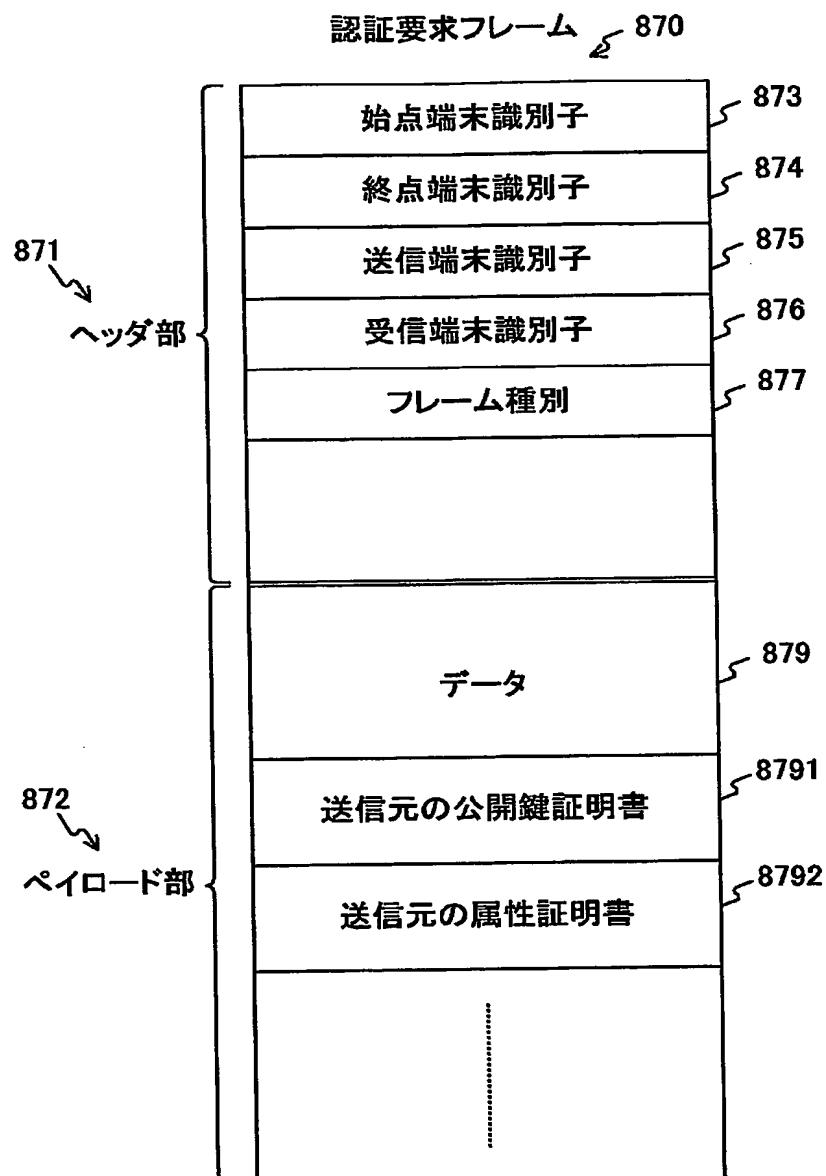
【図9】



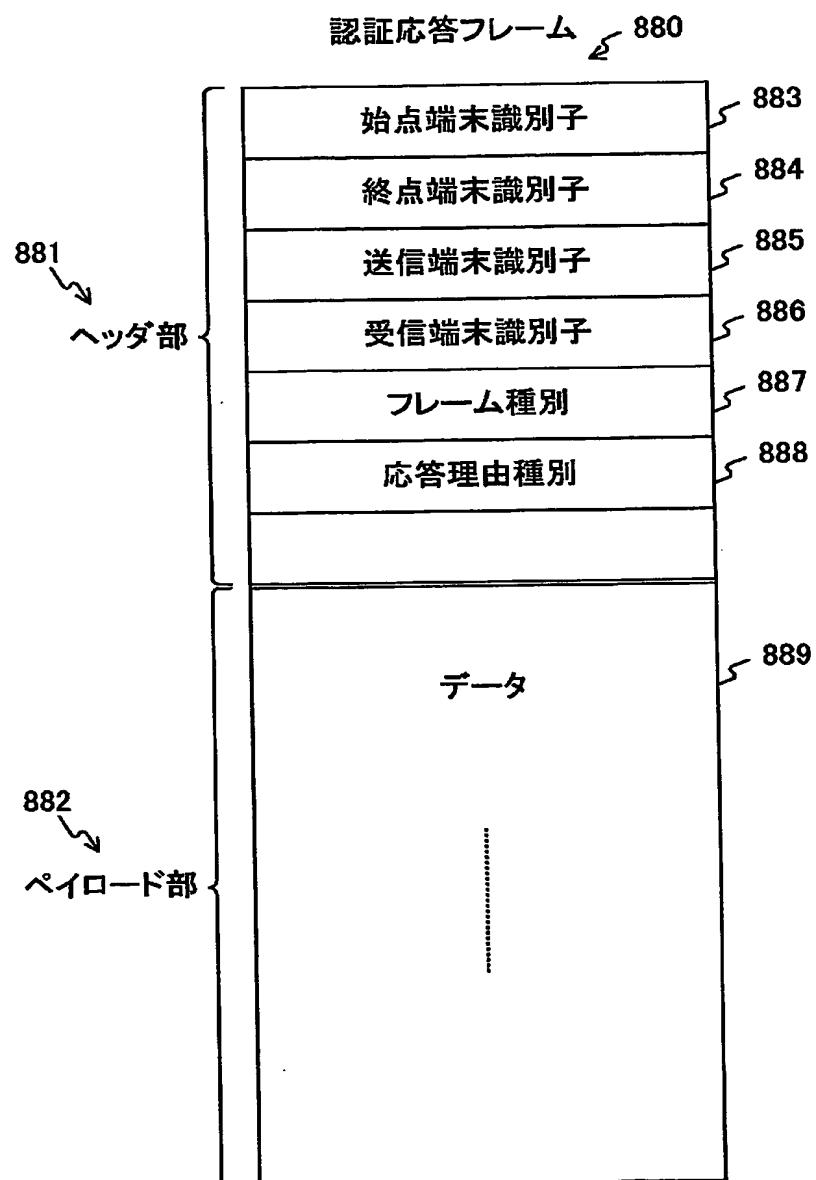
【図10】



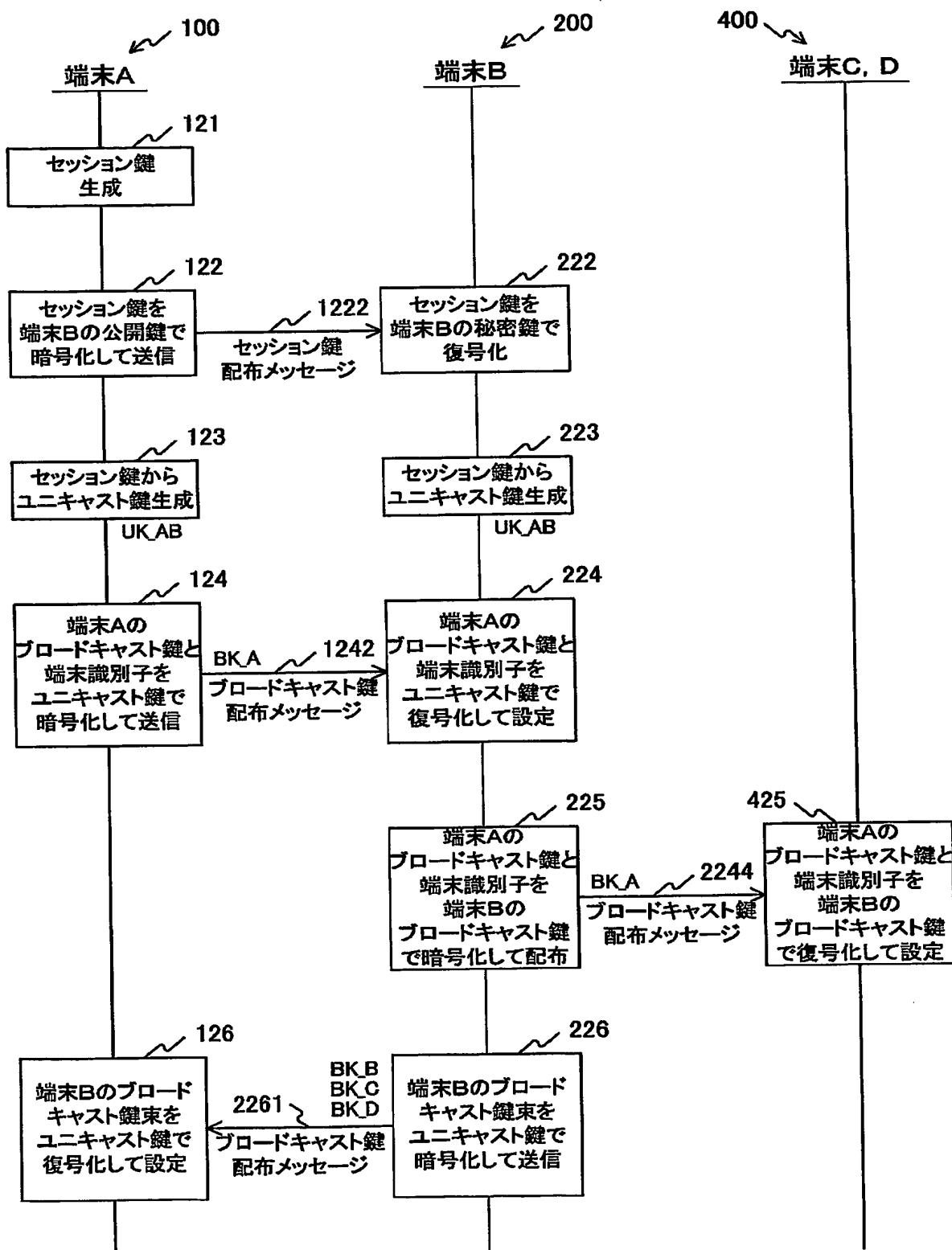
【図11】



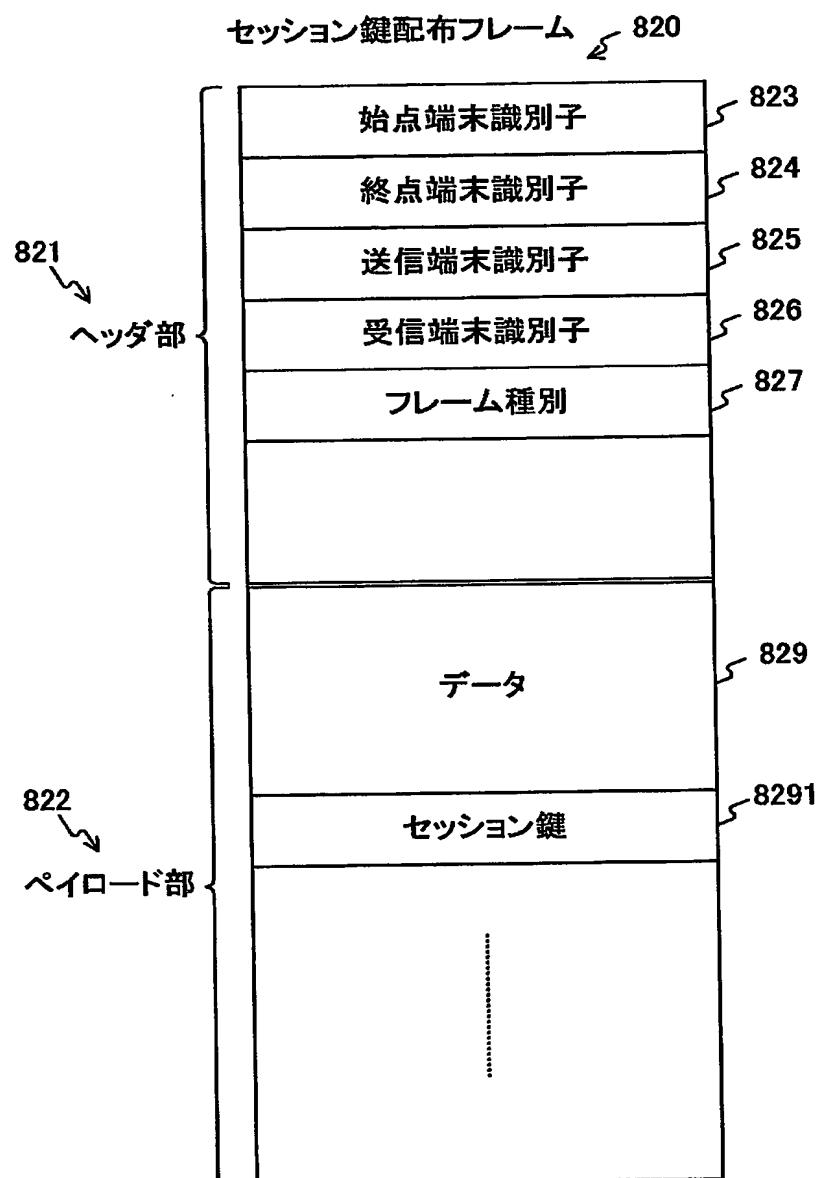
【図12】



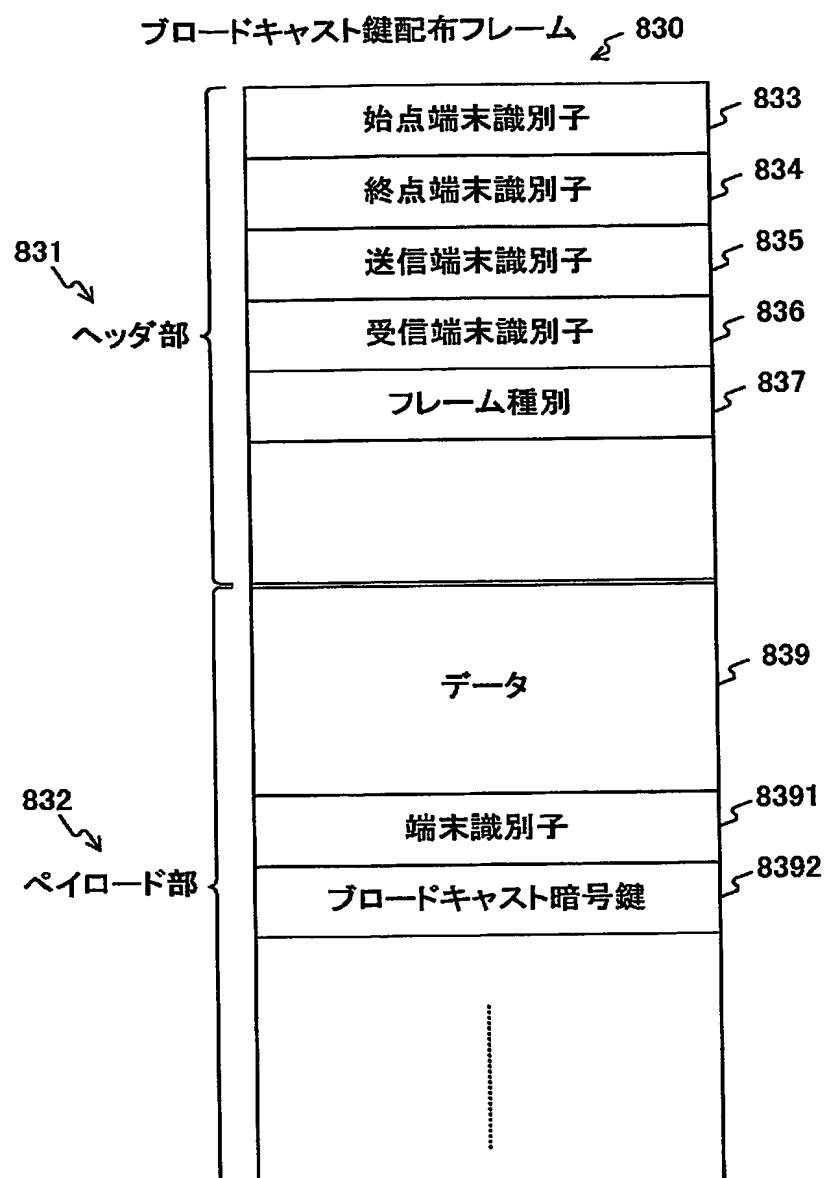
【図13】



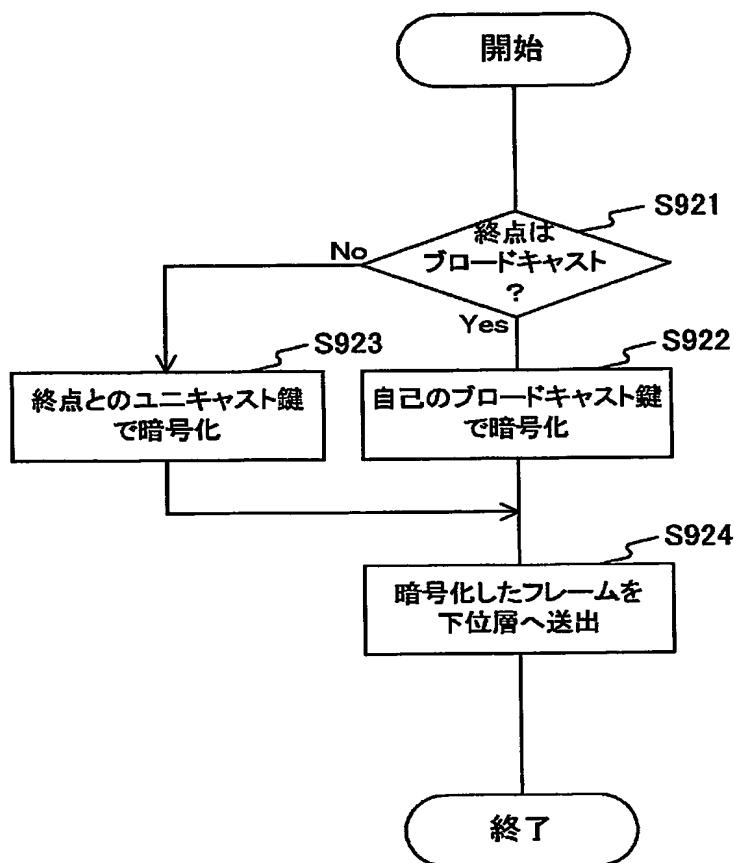
【図14】



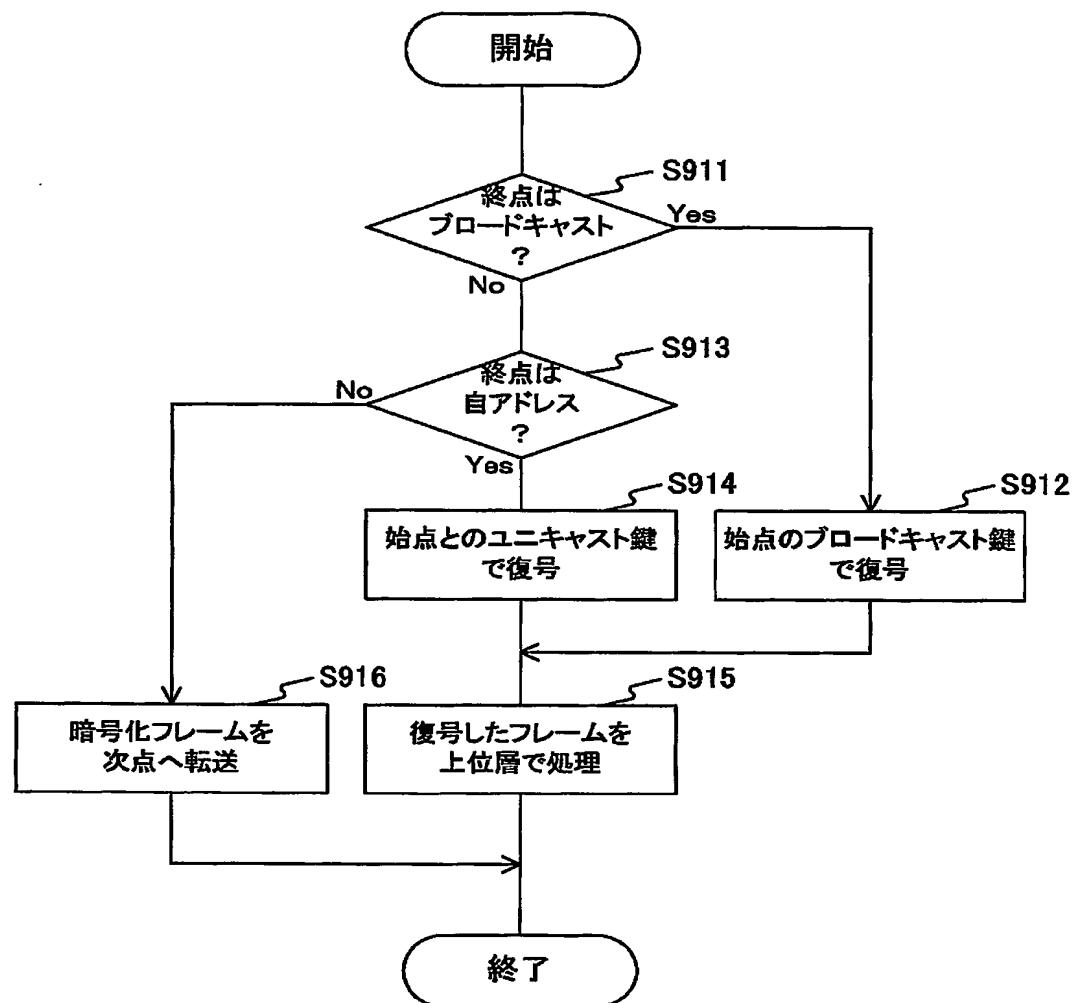
【図15】



【図16】



【図17】



【書類名】 要約書

【要約】

【課題】 無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行う。

【解決手段】 無線アドホック通信システムにおける各端末は暗号鍵管理リストテーブル660を備える。この暗号鍵管理リストテーブル660では、MACアドレス等の端末識別子661に関連付けられて、その端末識別子661により識別される端末との間のユニキャスト通信に用いられるユニキャスト暗号鍵662およびその端末識別子661により識別される端末がブロードキャスト通信を行う際に用いられるブロードキャスト暗号鍵663が保持される。これにより、ブロードキャスト通信を行う端末毎にブロードキャスト暗号鍵が設けられ、ブロードキャスト暗号鍵の管理が各端末により自律分散して行われる。

【選択図】 図5

特願 2003-026543

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住所 東京都品川区北品川6丁目7番35号
氏名 ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.